The official voice of the Air Force Research Laboratory

news@afrl

CIO Topics

Fall 2000

Volume II, Issue 3

OPSEC: Protecting technology, our business ‘marrow’

by Mark Rogers, Operations Security

Operations Security (OPSEC) is an integral part on AFRL functions. It goes hand in hand with other security disciplines to support the protection of technology — the marrow of our business.

OPSEC is an on-going system of periodic checks and balances to ensure critical information is protected for our laboratory operations and warfighting customers. It applies to all AFRL products that are generated as a result of a warfighter technology need or shortfall. This also includes briefings, conferences, symposiums, lectures and other activities related to AFRL.

Historically, OPSEC focus has been placed within the operations arena and OPSEC plays an important role in an operational wing. However, Wright-Patterson AFB also has many organizations that provide oversight and day-to-day program management in research, development, manufacturing, deployment and ongoing logistics support of weapons systems. Within AFRL, the primary mission of many activities is acquisition-related. This environment is not routinely thought of as needing an OPSEC program, but these are not routine activities!

Adversaries are highly interested in trying to dull the USAF’s sharp technological edge by methods that may directly target Wright-Patterson organizations and their defense contractors. Let’s explore some methods that may require a closer OPSEC look.

One Person’s Trash is Another Person’s Treasure

Who was it that said computers are creating a paperless society? This could not be further from the truth. The convenience of printing countless drafts, sending documents as attachments, and the “forward” icon as an e-mail feature has created a mountain of paper products. Laser printers are abundant, and documents can be created with ease. These all contribute to tons of paper. Let’s face it…it is much easier to create paper products now than it was 15 years ago.

Much of what is being created can be unclassified sensitive information or For Official Use Only (FOUO) information that could possibly lead an adversary to development of your activity-specific Critical Information. Current regulations allow FOUO information to be “torn into pieces” (as opposed to shredded). Ask yourself if the risk of this perfectly legal procedure for the destruction of FOUO is really appropriate for your organization. It is a balance between vulnerability and risk. A number of organizations elect to destroy or shred all paper products.

The Internet as a Major OPSEC Concern

Web pages have become a means of transmitting information quickly to the customer. Web pages require appropriate review prior to posting. If your organization has a web page, is the OPSEC Program Manager for your activity, involved in the review process? If they aren’t now, they should be.

Non-public access web pages that contain sensitive unclassified or FOUO information must be properly protected through the use of firewalls, passwords and/or encryption. AFI 33-119, Electronic Mail (E-Mail) Management and Use, states the following:

“Users of E-mail systems must stay constantly aware of communications systems vulnerabilities and the need to safeguard “critical information,” OPSEC indicators, and sources of such information. As a minimum, you must encrypt “critical information,” OPSEC indicators, and sources of such information before transmission across the Internet.”

As information technology become faster and interconnectivity becomes larger, the system is only as good as its weakest link. The potential information sinkhole that can be created due to poor OPSEC could literally put systems and lives on the line. Computers are definitely a growth industry for OPSEC.

Restricted Controlled or Open Access?

As trivial as it may sound, office techniques in place within active program’s can make a difference in mitigating potential vulnerabilities. Public access through some areas (public…meaning personnel outside your organization) could become an OPSEC issue. Minimizing or negating through-traffic within the office also may be in order. Within an open office environment, personnel should be in the habit of routinely challenging folks that aren’t part of the organization and appear to be walking through.

Clean Desk or Adversary Gold Mine?

A clean desk policy helps to ensure potential OPSEC indicators don’t become targets of opportunity. Test schedules, TDY itineraries, ongoing technical/contractual documents all may have potential value and are the type of information normally accessible on the desktop.

OPSEC Synergy

In OPSEC, the sum of the parts always is worth more than the whole. Collecting seemingly benign OPSEC indicators could potentially expose major weapons system vulnerabilities. This synergy works both ways. Having a viable organization OPSEC program includes paying attention to otherwise minor details, as minor details can add up exponentially. Enforcing a number of OPSEC initiatives has a combined effort that will pay dividends by mitigating vulnerabilities.

With proper support from AFRL members, critical information and technology will be protected and our technological advantage will be uncompromised. **@**